



RECEIVED

AUG 30 2019

CONSUMER PROTECTION

August 28, 2019

Attorney General Gordon MacDonald
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

On behalf of our client, the National Education Association (the “NEA”), we write to provide you with this preliminary notification of an incident that may have affected the personal information of two (2) New Hampshire residents. The NEA recently learned of an incident involving a service provider, which may have affected the security of some of the personal information of plan participants in the Employees’ Retirement Plan of the National Education Association of the United States (the “Retirement Plan”).

The NEA, on behalf of the Retirement Plan, engages a service provider, Calibre CPA Group (“Calibre”), to perform financial audits of the Retirement Plan. In support of a recent audit, Calibre stored certain tax forms containing plan participant personal information on its servers. On August 1, 2019, Calibre contacted the NEA to report that Calibre had suffered a cyber attack that resulted in unauthorized access to the server on which these tax forms are stored. Calibre is unable to confirm whether the bad actors may have viewed any specific data on the server, but they were able to determine that the information present on the server at the time of the incident, which could potentially have been viewed, included certain plan participants’ first and last names and Social Security numbers.

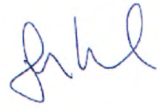
Our understanding from Calibre is that it has taken steps to further strengthen the security of its systems as a result of this incident, as well as that it has notified law enforcement. Calibre will also be offering affected plan participants a two-year subscription for identity theft protection and credit monitoring services from Kroll at no charge.

Calibre will begin notifying affected plan participants in the next few days. A copy of the letter they will be sending is attached for your reference. The NEA is also sending a pre-notification letter to affected plan participants so that they know to expect a notification from Calibre.

Calibre will soon be sending you the official notification required by N.H. Rev. Stat. § 359-C:19.

Should you have further questions about this matter, please do not hesitate to contact me at 202-706-5216 or jason@zwillgen.com.

Sincerely,

A handwritten signature in blue ink, appearing to read 'JRW'.

Jason R. Wool



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Calibre CPA Group (“Calibre”) writes to notify you of a recent incident that may affect the security of some of your personal information. We are providing you with information on the event and measures we have taken since discovering the incident.

What Happened? Calibre recently became aware of suspicious activity related to certain employee email accounts, as well as one of our computer servers. We immediately launched an investigation to determine the full nature and scope of the email activity and what information may have been affected. With the assistance of computer forensics experts, we learned that one of our computer servers as well as certain Calibre employee email accounts were accessed without authorization between March 11, 2019 and May 7, 2019.

Working with these third-party experts, we undertook a comprehensive review of the impacted email accounts and impacted server to determine if they contained personal information and received confirmation of the scope of potentially impacted individuals on June 26, 2019. However, based on the information contained within the affected data, we still lacked complete address information related to individuals and were unable to adequately identify any potential business partners from whom the information originated. Calibre subsequently undertook a lengthy internal review of our systems to determine this information, and later determined that information related to you was accessible during the period of potential compromise.

We are notifying you in an abundance of caution because your information was present and potentially accessible at the time of the incident. Calibre functions as a full-service accounting and advisory firm, offering audit, advisory, and general accounting services. It was through our business relationship with <<b2b_text_2>> that your information was contained within our impacted systems.

What Information Was Involved? Calibre cannot confirm specifically what information, if any, was viewed by the unauthorized individual. However, Calibre’s investigation confirmed the information present at the time of the incident may include your <<b2b_text_1>>.

What We Are Doing. Information privacy and security are among our highest priorities. Calibre has strict security measures in place to protect information in our care. Upon learning of this incident, Calibre took steps to confirm and further strengthen the security of our systems. As a precautionary matter, Calibre also notified law enforcement and provided relevant regulatory notices.

We are notifying potentially affected individuals, including you, so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We also secured the services of Kroll to provide identity monitoring services at no cost to you for two (2) years. For more information on these services, please review the enclosed “Steps You Can Take to Protect Against Identity Theft and Fraud.”

What You Can Do. You may review the information contained in the enclosed “Steps You Can Take to Protect Against Identity Theft and Fraud.” You may also activate to receive the identity monitoring services we are making available to you as we are unable to activate these services on your behalf.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-833-496-0188 which can be reached Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. You may also write to us at ATTN: Cyber Security, Calibre CPA Group, PLLC, PO Box 30380, Bethesda, Maryland 20824.

Calibre takes the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Calibre CPA Group, PLLC

Steps You Can Take to Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit enroll.idheadquarters.com to activate and take advantage of your identity monitoring services.

*You have until **November 21, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There are XXX Rhode Island residents impacted by this incident.](#)



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.